DEPARTAMENTO
DE COMPUTACION

Facultad de Ciencias Exactas y Naturales - UBA

Trabajo Práctico III

System Programming - Zombi defense

Organización del Computador II

Segundo Cuatrimestre de 2014

Integrante	LU	Correo electrónico
Aldasoro Agustina	86/13	agusaldasoro@gmail.com
Rey Maximiliano	37/13	rey.maximiliano@gmail.com
Tirabasso Ignacio	718/12	ignacio.tirabasso@gmail.com

Facultad de Ciencias Exactas y Naturales
Universidad de Buenos Aires
Ciudad Universitaria - (Pabellón I/Planta Baja)
Intendente Güiraldes 2160 - C1428EGA
Ciudad Autónoma de Buenos Aires - Rep. Argentina
Tel/Fax: (54 11) 4576-3359
http://www.fcen.uba.ar

1. Ejercicio 1

a) Tabla de descriptores de la GDT.

Al momento de armar la GDT, acorde a lo dispuesto en el enunciado, dejamos las primeras siete entradas de la tabla de descriptores libres. Luego, a partir de la posición 8 dejamos los descriptores de segmento pedidos: código y datos nivel 0 y código y datos nivel 3.

Armamos los cuatro segmentos de la GDT, llamándolos:

```
[GDT_IDX_DATA_0] = (gdt_entry) ;
[GDT_IDX_DATA_3] = (gdt_entry) ;
[GDT_IDX_CODE_0] = (gdt_entry) ;
[GDT_IDX_CODE_3] = (gdt_entry) ;
```

A los cuatro les seteamos el mismo *límite*: **0x26EFF** y la misma *base* en **0**, de este modo los cuatro descriptores de segmento direccionan a los primeros *623MB* de memoria. El *segment type* varía depende el segmento: CODE_0: **0x0A** (code execute/read), CODE_3: **0x0F** (code execute/read, conforming, accesed), DATA_0 y DATA_3: **0x02** (data read/write). El *Descriptor type* va en todos para system, por lo tanto es **0**. El *Descriptor privilege level* coincide con el nombre del descriptor (**0** para CODE_0 y DATA_0; **3** para CODE_3 y DATA_3). El bit de *Present* va para todos en **1** y los bit de *Available for use by system software* y *l* van para todos en **0**. El bit de *Default operation size* va para todos en **1** porque es un código de 32bits. El bit de *Granularity* va para todos en **1**.

b) Pasaje a modo protegido y seteo de la pila del kernel.

Para pasar a modo protegido los pasos que debemos llevar a cabo son:

- ▷ Completar la GDT (resuelto en el inciso A).
- ▷ Deshabilitar interrupciones (para ello se ejecuta la instrucción *cli*).
- ▷ Habilitar A20 (en nuestro caso se resuelve haciendo *call habilitar_A20*).
- ▷ Cargar el registro GDTR con la dirección base de la GDT (lo hacemos con la instrucción *lgdt [GDT_DESC]* la etiqueta GDT_DESC apunta al descriptor de la GDT en el código).
- ▷ Una vez hecho esto, estamos en condiciones de setear el bit PE del registro CR0 (debemos hacer: *mov eax,cr0 ; or eax,1 ; mov cr0,eax*).
- ▷ Lo siguiente a realizar es el *jump far* a la siguiente instrucción (utilizamos el selector de segmento *0x50* y de offset la etiqueta *modo_protegido* por que el selector es 0x50??).
- ▷ Una vez ya en modo protegido, nos encontramos trabajando en 32 bits y ahora es cuando cargamos los registros de segmento (a los registros *es, ds, ss y gs* les asignamos el valor de *0x40* y al registro *fs* le asignamos el valor *0x60* aca habría que poner el porque de estos valores??).

Para setear la pila del kernel en la dirección 0x27000 debemos llevar a cabo la siguiente instrucción:

```
mov ebp, 0x27000
```

c) Segmento adicional que describe el área de la pantalla en memoria que puede ser utilizado sólo por el kernel.

HELP! aca no se que ponerrrrrrrr

```
; Cambiar modo de video a 80 X 50
mov ax, 0003h
int 10h ; set mode 03h
xor bx, bx
mov ax, 1112h
int 10h ; load 8x8 font
```

d) Rutina que se encarga de limpiar la pantalla y pintar el área del mapa

En este punto debemos establecer un fondo de color verde, junto con las dos barras laterales para cada uno de los jugadores (una roja y otra azul). Para esto, debemos contar con una función que limpie la pantalla en un primer momento: *clear_screen*.

La función ***clear_screen***, implementada en lenguaje C, se va a encargar de:

- ▷ Guardar en una variable local: *size* el tamaño de la pantalla (VIDEO_COLS * VIDEO_FILS).
- ▷ Luego va a hacer un while desde *0* hasta *size* que, empezando por la dirección donde está almacenada la memoria de video, vaya guardando el caracter que es todo negro.

De este modo, logramos hacer que toda el área de la pantalla quede “pintada” de negro.

En segunda instancia, armamos la función *print_map*. La función ***print_map***, también implementada en lenguaje C, con el fin de pintar el área del mapa con los colores deseados, posee el siguiente comportamiento:

- ▷ En un primer momento, llama a la función *clear_screen*.
- ▷ Se arman cuatro variables locales: blue, red, green y black. Cada una de ellas es un caracter completamente de su color.
- ▷ Mediante dos *fors* anidados recorremos toda el área del mapa, y dependiendo de la posición en la que se encuentre es el color que le va a ser asignado (rojo a las primeras dos columnas de la izquierda, azul a las últimas dos, negro a las últimas cinco filas y el resto en verde).

Luego este código fue complejizado para que pueda imprimir los puntos de los jugadores y sus respectivos puntajes por zombie tal cual debe ser cuando comienza el juego.

2. Ejercicio 2

ESTO HAY QUE HACERLO!!!!!!!!

3. Ejercicio 3

Limpiar el buffer de video es hacer clear_screen???... Asumo que sí.

a) Implementación completa de print_map.

En el ejercicio 1 ya habíamos logrado armar **clear_screen** y **print_map**, esta última contaba con una funcionalidad acotada. Sólo armaba cuatro bloques de colores. Ahora lo que vamos a hacer es extender la función **print_map** para que escriba los puntos de los jugadores y marque el estado de los zombies, tal como aparece en la *figura 9* del enunciado.

La función print_map la vamos a extender sumándole las siguientes instrucciones:

- Debemos armar los *cuadrados de puntaje* para el jugador rojo y para el jugador azul. Nos movemos entre las últimas cinco filas, desde la columna 35 hasta la 39 se pintan con el caracter completamente rojo y desde la columna 40 hasta la 44 se pintan con el caracter completamente azul.
- Escribimos en el centro de cada cuadrado el puntaje inicial: 0. Para ello creamos dos caracteres que sean 0 y cada uno con los atributos necesarios para que sean: fondo rojo, letra blanca y fondo azul, letra blanca.
- Luego escribimos la cantidad de zombies restantes, para lo cual se utilizan dos caracteres idénticos a los mencionados arriba. Estos puntajes se ubican cada uno a un costado de su cuadrado respectivo.
- Por último, resta escribir el estado de los zombies. Generamos un char* que sean todos los números de zombies y dándole formato de fondo negro, caracter blanco los copiamos dos veces: uno para el jugador azul y otro para el jugador rojo. Como todos los zombies se encuentran disponibles, generamos otro char* que sean diez 'x' y ubicamos en su posición correspondiente uno que posea los atributos de fondo negro, caracter azul y otro de fondo negro, caracter rojo.

Con el objetivo de hacer que lo descripto anteriormente sea una tarea más simple contamos con las funciones: *print_string* y *get_format*.

La función **print_string** recibe una posición en el mapa (x,y), un char* con el texto que queremos imprimir en pantalla y un short con los atributos deseados. PONER ALGO DE AVOID PRINT BUG. Dentro de un *for* que recorre horizontalmente la posición en memoria a partir de la posición (x,y), se va avanzando el char* y en cada iteración se le asigna a esa posición de memoria el char actual con los atributos pasados por parámetro.

La función **get_format** es una función simple la cual recibe como parámetro los atributos deseados y los devuelve con el formato de un sólo char, que es el que debemos utilizar.

```
unsigned char getFormat(unsigned char fore_color, char fore_bright, unsigned char back_color,
                        char blink) {
    return fore_color | fore_bright | back_color | blink;
}
```

b) Rutinas encargadas de inicializar el directorio y tablas de páginas para el kernel.

Para poder mapear las direcciones 0x00000000 a 0x003FFFFF es necesaria una sola entrada en el Page Directory. En un primer momento, se crea un puntero a Page Directory en la dirección 0x27000. Se limpian las 1024 entradas del Page Directory poniendo todos sus bits en 0.

Luego, a la primera entrada del Page Directory (índice: 0) se le asigna como base 0x28. Se le asigna permiso de escritura y lectura con su bit de presente seteado, como es de Kernel es de nivel 0.

Para que todo esto funcione y el primer índice del Page Directory apunte a un Page Table válido, se debe crear un Page Table en la posición 0x28000 en memoria. En esta misma se completan todos los índices (ya que es lo que ocupa el rango pedido para el Kernel) direccionándolos desde la posición 0x0 en memoria, aumentando en uno acorde aumenta el índice. Todos tienen permiso de escritura con el bit de presente seteado, como es de Kernel es de nivel 0.

c) Código necesario para activar paginación.

Como ya contamos con un directorio de páginas y una tabla de páginas estamos en condiciones de activar paginación.

Como para esto debemos poner en cr3 la base del directorio de páginas y limpiar los bits PCD y PWT del mismo, basta con asignarle a cr3 el valor de 0x27000. De este modo la base queda en 0x27 y los bits limpios. Es correcto esto?

Por último resta setear el bit PG del cr0, lo hacemos mediante un or.

4. Ejercicio 4

a) inicializar_mmu.

Para administrar la memoria en el área libre, tenemos un contador de páginas utilizadas denoninándolo *páginas*. Luego contamos con las funciones *get_page_directory* y *get_page_table* las cuales nos brindan un nuevo page directory o una nueva page table correspondientemente.

Todo esto aca del punto A esta re turbio...mirar que onda... ACA HAY QUE PONER GET_PAGE_TABLE Y GET_PAGE_DIRECTORY???

b) mmu_inicializar_dir_zombi

La rutina *mmu_inicializar_dir_zombi* se encarga de inicializar un directorio de páginas y tablas de páginas para una tarea, respetando la figura 6. Copia el código de la tarea a su área asignada, es decir la posición indicada por el jugador dentro del mapa y mapea dichas páginas a partir de la dirección virtual 0x08000000(128MB).

Este punto B tambien esta re turbio...

c) Mapear y Des-Mapear página.

La rutina *mmu_mapear_página* permite armar toda la estructura necesaria para que, dada una dirección virtual, un puntero a Page Directory, una dirección física y los atributos deseados (lectura/escritura y nivel); se mapee la dirección virtual a la física.

El comportamiento de la función **mmu_mapear_página** consiste en :

- Obtener el offset del Page_directory (*directory*) shifteando a la derecha 22 bits la dirección virtual pasada por parámetro.
- Obtener el offset del Page_table (*table*) shifteando a la derecha 12 bits la dirección virtual pasada por parámetro luego de haberle hecho un *and* con 0x003FF000 así obtengo sólo los bits de interés.
- Si el índice *directory* del Page Directory tiene el bit presente = 0, entonces debemos setear la base obteniendo una nueva Page Table (con la función get_page_table), dándole permismos de escritura y nivel acorde a lo pasado por parámetro y seteando el bit de presente.
- Obtener el puntero a la Page Table (*pt*), accediendo al índice *directory* del Page Directory pasado por parámetro, lo shifteamos a la izquierda 12 bits así tenemos la dirección de la página donde se encuentra la Page Table.
- En el índice *table* de la Page Table apuntada por *pt* le asignamos la dirección física pasada por parámetro shifteada a la derecha 12 bits, asignándole permisos de lectura/escritura acorde y nivel a lo pasado por parámetro y seteando el bit de presente.
- Por último, ejecutamos *tlbflush* para que se invalide la cache de traducción de direcciones.

A veces, vamos a necesitar des-mapear una página para que, bajo el cr3 actual, no se tenga más permiso de acceso a la misma. Por este motivo, contamos con la función *mmu_unmapear_pagina*.

La función **mmu_unmapear_pagina** va a recibir como parámetro una dirección virtual y el cr3 actual. El comportamiento de esta función, si el bit de presente del Page Directory al que apunta al cr3 está seteado, va a consistir en el simple acceso al Page Directory apuntado por el cr3, accediendo al índice descripto en la dirección virtual pasada por parámetro. Luego dirigirse al Page Table apuntado por este, accediendo al índice que se encuentra en la dirección virtual y una vez ahí limpiar el bit de presente. En otro caso, no es necesario tomar ninguna acción.

5. Ejercicio 5

a) Entradas necesarias en la IDT.

Completamos las entradas necesarias en la IDT para asociar una rutina a la interrupción del reloj, otra a la interrupción de teclado y por último una a la interrupción de software 0x66. Es decir las posiciones 32, 33 y 102.

Las primeras dos van a ser de privilegio 0 y la última de privilegio 3, asignándoselo mediante sus atributos.

HASTA ACA LLEGUE, NO DOY FE DE LO DE ABAJO. IGUAL ARRIBA TAMBIEN HAY ANOTACIONES EN ROJO!

b) A continuación, la rutina asociada a la interrupción del reloj, para que por cada tick llame a la función screen próximo reloj. La misma se encarga de mostrar cada vez que se llame, la animación de un cursor rotando en la esquina inferior derecha de la pantalla.

```
;; Rutina de atención del RELOJ

global _isr32
_isr32:
    pushad
    call proximo_reloj   ; Ya definida en isr.asm
    call proximo_indice  ;Devuelve el próximo índice en la GDT a ejecutar

    cmp ax,0
    je .nojump

    mov [sched_tarea_selector], ax
    call fin_intr_pic1
    jmp far [sched_tarea_offset]
    jmp .end

.nojump:
    call fin_intr_pic1

.end:
    ; switchear tareas.
    popad
    iret
```

c) Ahora, la rutina asociada a la interrupción de teclado de forma que si se presiona cualquiera de las teclas a utilizar en el juego, se presenta la misma en la esquina superior derecha de la pantalla.

```
;; Rutina de atención del TECLADO

global _isr33
extern printf
extern print_int
extern handle_keyboard_interrumption
_isr33:
    pushad
    xor eax,eax
    in al, 0x60

    mov dword [esp], eax
    call handle_keyboard_interrumption

    mov dword  [esp + 0x], 0
    mov dword [esp + 0xc], 67
    mov dword [esp + 0x8], keyboard_str
    mov dword [esp + 0x4], eax
    call printf    ;función implementada por nosotros

    call fin_intr_pic1
    popad
    iret
```

d) Escribimos la rutina asociada a la interrupción 0x66 para que modifique el valor de eax por 0x42.

```
;; Rutina de atención 0x66

global _isr66
_isr33:

    mov eax,0x42

    iret
```

6. Ejercicio 6

a) Definimos tres entradas en la GDT que consideramos necesarias para ser usadas como descriptores de TSS: una para ser utilizada por la tarea inicial, otra para la tarea actual y una última para la tarea siguiente.

b) Completamos la entrada de la TSS de la tarea Idle con la información de la tarea Idle. La tarea Idle se encuentra en la dirección 0x00016000. La pila se alojará en la misma dirección que la pila del kernel y será mapeada con identity mapping. Esta tarea ocupa 1 pagina de 4KB y debe ser mapeada con identity mapping. Además la misma comparte el mismo CR3 que el kernel.

```
void tss_inicializar() {
    int i = 0;
    while(i < CANT_ZOMBIS) {
        inUseA[i] = 0;
        inUseB[i] = 0;
        i++;
    }
    currentZombieA = 0;
    currentZombieB = 0;

    // inicializar tss_idle
    tss_inicializar_tarea_idle();

    memcpy(&tss_idle, &tss_inicial, sizeof(tss));
    memcpy(&tss_idle, &current_task, sizeof(tss));
    memcpy(&tss_idle, &next_task, sizeof(tss));

    gdt[GDT_INITIAL_TSS].base_31_24 = ((u32) (&tss_inicial) & 0xFF000000) >> 24;
    gdt[GDT_INITIAL_TSS].base_23_16 = ((u32) (&tss_inicial) & 0x00FF0000) >> 16;
    gdt[GDT_INITIAL_TSS].base_0_15  = (u32) (&tss_inicial) & 0x0000FFFF;

    gdt[GDT_CURRENT_TSS].base_31_24 = ((u32) (&current_task) & 0xFF000000) >> 24;
    gdt[GDT_CURRENT_TSS].base_23_16 = ((u32) (&current_task) & 0x00FF0000) >> 16;
    gdt[GDT_CURRENT_TSS].base_0_15  = (u32) (&current_task) & 0x0000FFFF;
}
```

```
void tss_inicializar_tarea_idle() {

    tss_idle = (tss) {};

    tss_idle.eip = 0x00016000;
    tss_idle.cr3 = 0x27000;

    tss_idle.ebp = 0x27000;
    tss_idle.esp = 0x27000;

    tss_idle.es = 0x40;
    tss_idle.ds = 0x40;
    tss_idle.ss = 0x40;
    tss_idle.gs = 0x40;
    tss_idle.cs = 0x50;

    tss_idle.eflags = 0x202;
    tss_idle.iomap = 0xffff;
}
```

d) Código necesario para ejecutar la tarea Idle, es decir, saltar intercambiando las TSS, entre la tarea inicial y la tarea Idle:

```
idle:
    .loopear:
        inc dword [numero]
        cmp dword [numero], 0x4
        jb .imprimir

    .reset_contador:
        mov dword [numero], 0x0

    .imprimir:
        ; Imprimir 'reloj'
        mov ebx, dword [numero]
        add ebx, message1
        imprimir_texto_mp ebx, 1, 0x0f, 49, 76
        mov ebx, chirimbolo_open
        imprimir_texto_mp ebx, 1, 0x0f, 49, 76-1
        mov ebx, chirimbolo_close
        imprimir_texto_mp ebx, 1, 0x0f, 49, 76+1

    jmp .loopear
```

7. Ejercicio 7

c) Se muestra la rutina de la interrupción 0x66, para que implemente el servicio mover según se indica en la sección 3.1.1.

```
global _isr66
extern movimiento
_isr66:
    pushad

    push dx
    push esi
    push edi
    push eax
    call movimiento

    popad
    iret
```